PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-298974

(43)Date of publication of application : 24.10.2000

---

(51)Int.Cl. G11B 27/00
G06F 12/14

---

(21)Application number : 11-103130 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 09.04.1999 (72)Inventor : TAKEI HIDEAKI
SONEOKA AKINAO

---

(54) INFORMATION RECORDING METHOD CAPABLE OF MOVING INFORMATION MADE PECULIAR TO MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize an information recording method which moves information made peculiar to a storage medium to another storage medium while preventing the wrong use.

SOLUTION: When contents A141 are moved from a storage medium A1 to a storage medium B1, a contents read means 51 records read contents ID.A1421 in an ineffective contents ID management table of the storage medium A1, and contents data A1422 is recorded in the storage medium B1 as contents B142 through a generalizing means 52, a peculiarity making means 54, and a contents recording means 55, and contents A142 are deleted from the storage medium A1.

LEGAL STATUS [Date of request for examination] 13.03.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3773697
[Date of registration] 24.02.2006
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] While having the RAM field which is a storage region rewritable the WAO field which is a storage region which can be written in only at once, and any number of times It is the information record approach which records information to the storage media in which the media ID which are peculiar identifiers, and which are not rewritable are written for every media. In case the purpose information is recorded on said storage media Search the content ID which can be used within said storage media, and said Media ID and said content ID are combined. Generate media content ID, and proper-ize said purpose information by said media content ID, and contents data are generated. The information record approach which makes movable media proper-ized information characterized by recording the contents which made the group said content ID and said contents data on said RAM field of said storage media.

[Claim 2] The invalid content ID managed table for managing the content ID which cannot be used in said storage media from now on is recorded on said WAO field. In case said contents currently recorded on said storage media are read and said purpose information is acquired from these read contents Check, and when recorded, whether the content ID of said contents read from said storage media is recorded on said invalid content ID managed table When acquisition processing of the purpose information is stopped and the content ID of said contents is not recorded on said invalid content ID managed table Combine said Media ID and said content ID, generate media content ID, and the contents data of said contents are generalized by this generated media content ID. The information record approach which makes movable media proper-ized information according to claim 1 characterized by acquiring said purpose information.

[Claim 3] The invalid content ID managed table for managing the content ID which cannot be used in said storage media from now on is recorded on said WAO field. The available content ID managed table for managing the content ID which can be used in said storage media is recorded on said RAM field. In case said contents are moved to the 2nd storage media from the 1st storage media After checking that read said contents from said 1st storage media, and the content ID of these read contents is not recorded on said invalid content ID managed table of said 1st storage media While recording this content ID on this invalid content ID managed table Delete this content ID from said available content ID managed table of said 1st storage media, and the 1st media ID of said 1st storage media and said read content ID of contents are combined. Generate the 1st media content ID and the contents data of said contents are generalized by this 1st media content ID. Acquire said purpose information and said

the 2nd Media ID and said content ID of storage media are combined. [2nd] Generate the 2nd media content ID, and proper-ize the purpose information acquired from said 1st storage media by said 2nd media content ID, and contents data are generated. The contents which made the group said content ID and said contents data are recorded on said RAM field of said 2nd storage media. The information record approach which makes movable media proper-ized information according to claim 1 characterized by eliminating said contents currently recorded on the RAM field of said 1st storage media.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention proper-izes information to the storage media which have the media ID which are peculiar identifiers for every media, reads this information proper-ized from storage media, and it relates to the information record approach which makes movable media proper-ized information that informational unjust use can be prevented accurately while it moves to the storage media of further others.

[0002]

[Description of the Prior Art] First, vocabulary called informational proper-izing and informational generalization is explained. Below, it expresses enciphering Data D by

the cryptographic key K as E (K, D).

[0003] In order to prevent unjust use, the approach using the private key made are shared between the equipment which records information or is used, and secret to a user is used well. This private key is called the equipment key R.

[0004] Furthermore, by proper-izing information to media, even if it copies information to other media, since information cannot be decrypted appropriately, by other media, it becomes possible to prevent unjust use. The one example is the approach which used the peculiar identifier for every media. The approach which used the peculiar identifier for every media is explained briefly below.

[0005] It is written in each media so that a peculiar identifier (media ID) can be beforehand rewritten for every media. Therefore, when there are two media, each media ID of these two media are not in agreement. When recording the purpose information C which is going to prevent unjust use to such media, Media ID (MI) are first enciphered with the equipment key R, and E (R, MI) is obtained. Media write in the encryption purpose information E (E (R, MI), C) which enciphers the purpose information C and is generated by making this into a cryptographic key.

[0006] On the other hand, when reading this purpose information C, the encryption purpose information E (E (R, MI), C) and Media ID (MI) which are recorded are read, MI is enciphered with the equipment key R, E (R, MI) is obtained, E (E (R, MI), C) can be decrypted by the ability making this into a decode key, and the purpose information C can be acquired.

[0007] At this time, the encryption purpose information currently recorded on a certain media A is copied to another media B, and it considers reading this encryption purpose information from Media B. At this time, the media ID of Media A (MIA) differ from the media ID of Media B (MIB). Therefore, since the key (E (R, MIA)) used for encryption differs from the key (E (R, MIB)) used for a decryption even if it is going to read the encryption purpose information copied to Media B as mentioned above, the purpose information cannot be read correctly. That is, this encryption purpose information is effective information only when recorded on Media A, and when recorded on other media, it turns into invalid information. This is called proper-ization to the media of the purpose information. By proper-izing information to media, it became impossible to use, even if it copies information to other media, and it has prevented unjust use.

[0008] Moreover, in order to generate the encryption purpose information E (E (R, MI), C), it is necessary to get to know the equipment key R other than Media ID (MI) and the purpose information C. On the contrary, in order to decrypt the encryption

purpose information E (E (R, MI), C), it is necessary to get to know the equipment key R other than Media ID (MI). Therefore, the encryption purpose information cannot be generated unjustly or the purpose information cannot be generated from the encryption purpose information just because Media ID were known, if the equipment key R was protected secretly.

[0009] As explained above, it becomes a powerful approach to proper-ize information to media realizing prevention of unjust use. Even if the information in media will be copied since information in media is proper-ized by the media if it has another way of speaking, it will not serve as a threat to the unjust use prevention approach. It is because it is completely meaningless when the proper-ized information becomes that which is decrypted appropriately and is meaningful only when recorded on the media, and recorded on other media. That is, in order to use the information proper-ized by media, it is necessary to own the media physically. The right using information is connected to possession of physical media.

[0010] Then, the purpose information will be expressed for it, if it proper-izes generating the proper-ized purpose information E (E (R, MI), C) from Media ID (MI) and the purpose information C by Media ID, and if the proper-ized purpose information is generalized by Media ID, it will express generating Media ID to the proper-ized purpose information and the purpose information.

[0011] It is satisfactory, when preventing unjust use even if the proper-ized information in media is copied by other media so that clearly from the above explanation. Therefore, a user can record the proper-ized information in media on another media, such as a hard disk and MO, as backup. If a user copies some of them to another record medium as backup and the information in a special and its storage media is deleted when a lot of information accumulates in storage media and the remaining memory capacity has decreased, he can increase the remaining memory capacity. What is necessary is just to return information to storage media from backup, if needed. The returned information can be used as effective information. Thus, it is very convenient for a user that a user can take and set informational backup without limit lawfully.

[0012] By the way, in order to use the information recorded on storage media by such conventional approach in order to use by other storage media, information will not be able to be moved, but a user will have forced inconvenience at the point. If it is allowed for this to have not said the thing of backup, to copy information to another media, and to use information on the another media, it has said that the room of unjust use is produced.

[0013] Informational migration is moving information from Media A to Media B. The user is convenient if the separate information included in two media can be summarized to one media, and it is necessary to move information at this time. From a viewpoint of preventing unjust use in informational migration, when moving information to Media B from Media A, I hear that important one prevents from that information in Media A is used later, and there is. That is, it can be said that informational migration is the activity of proper-izing [re] information proper-ized by Media A to Media B, and it is the activity which moves the right using the information connected to Media A, and is connected to Media B before migration.

[0014] In order to move between media, the following approaches are considered easily. The information by which it was first proper-ized in Media A is generalized. This generalized information is proper-ized to Media B, and it records on Media B. And the information by which it was proper-ized in Media A is eliminated. If a user is provided with such a function, migration of the proper-ized information between media is realizable for the time being.

[0015] However, it poses a problem that information in the media A which are not allowed use can use no longer certainly here. For example, before doing the activity of migration of a user, the case where the information in Media A is backed up beforehand is considered. After the activity of migration is completed, since the information in Media A is eliminated as mentioned above, to be sure in Media A, the information which moved does not remain. However, if backup is taken beforehand, and this backup will be copied to Media A again and will be returned, this information can be effective and can be used.

[0016] In the case of the simple storage media only recorded especially, it is difficult to develop the technique of preventing backup, although such unjust use can be prevented by forbidding backup. Furthermore, backup is a function convenient in itself above all, and it is very inconvenient to a user to forbid this.

[0017] As mentioned above, in a Prior art, when a user is provided with the function which moves the information in media to other media, it will become easy for a user to copy information unjustly and to use it.

[0018]

[Problem(s) to be Solved by the Invention] As mentioned above, when it is going to realize moving the information proper-ized by media to other media, there is a problem that unjust use will be easily performed by recopying backup to media after informational migration.

[0019] Although unjust use can be prevented by preventing backup, preventing

backup has the problem of spoiling a user's convenience.

[0020] The place which this invention was made in view of the above, and is made into the purpose is for offering the information record approach which makes movable media proper-ized information that unjust use of the information by the illegal copy can be prevented accurately, making backup possible by moving the information proper-ized by storage media to different storage media.

[0021]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention according to claim 1 While having the RAM field which is a storage region rewritable the WAO field which is a storage region which can be written in only at once, and any number of times It is the information record approach which records information to the storage media in which the media ID which are peculiar identifiers, and which are not rewritable are written for every media. In case the purpose information is recorded on said storage media Search the content ID which can be used within said storage media, and said Media ID and said content ID are combined. Media content ID is generated, said purpose information is proper-ized by said media content ID, and contents data are generated, and let it be a summary to record the contents which made the group said content ID and said contents data on said RAM field of said storage media.

[0022] If it is in this invention according to claim 1, combine Media ID and content ID and media content ID is generated. In order to record the contents which proper-ized the purpose information by media content ID, generated contents data, and made content ID and contents data the group on storage media, While being able to proper-ize the purpose information by the result of having enciphered Media ID by content ID Moreover, it is also possible by preparing another contents key beforehand, enciphering contents with a contents key, and proper-izing a contents key as purpose information to mitigate processing of encryption of contents.

[0023] Moreover, this invention according to claim 2 records the invalid content ID managed table for managing the content ID which cannot be used in said storage media from now on in invention according to claim 1 on said WAO field. In case said contents currently recorded on said storage media are read and said purpose information is acquired from these read contents Check, and when recorded, whether the content ID of said contents read from said storage media is recorded on said invalid content ID managed table When acquisition processing of the purpose information is stopped and the content ID of said contents is not recorded on said invalid content ID managed table Let it be a summary to combine said Media ID and

said content ID, to generate media content ID, to generalize the contents data of said contents by this generated media content ID, and to acquire said purpose information.
[0024] If it is in this invention according to claim 2, when the content ID of contents is recorded on the invalid content ID managed table Stop acquisition processing of the purpose information, and when not recorded In order to combine Media ID and content ID, to generate media content ID, to generalize the contents data of contents by this media content ID and to acquire the purpose information, It becomes an invalid, and the purpose information on the contents currently recorded on the invalid content ID managed table can generalize contents data by the result of having enciphered Media ID by content ID further while it is unacquirable. In addition, although there is a possibility of making contents into the contents which have content ID other than original content ID by having not enciphered about the content ID contained in contents, and making content ID into another value unjustly, the proper-ized data are recorded with the value which contains content ID as contents data contained in contents, and it depends for contents data on content ID. In this case, as mentioned above, when reading contents data, in order to generalize contents data with the value containing ID which is not original content ID, the information acquired as a result of read-out turns into meaningless information instead of true honest information. Therefore, the information acquired even if it changes content ID from an original thing only becomes meaningless.
[0025] Furthermore, this invention according to claim 3 records the invalid content ID managed table for managing the content ID which cannot be used in said storage media from now on in invention according to claim 1 on said WAO field. The available content ID managed table for managing the content ID which can be used in said storage media is recorded on said RAM field. In case said contents are moved to the 2nd storage media from the 1st storage media After checking that read said contents from said 1st storage media, and the content ID of these read contents is not recorded on said invalid content ID managed table of said 1st storage media While recording this content ID on this invalid content ID managed table Delete this content ID from said available content ID managed table of said 1st storage media, and the 1st media ID of said 1st storage media and said read content ID of contents are combined. Generate the 1st media content ID and the contents data of said contents are generalized by this 1st media content ID. Acquire said purpose information and said the 2nd Media ID and said content ID of storage media are combined. [2nd] Generate the 2nd media content ID, and proper-ize the purpose information acquired from said 1st storage media by said 2nd media content ID, and contents data are generated. Let

it be a summary to eliminate said contents which record the contents which made the group said content ID and said contents data on said RAM field of said 2nd storage media, and are recorded on the RAM field of said 1st storage media.

[0026] If it is in this invention according to claim 3, in case said contents are moved to the 2nd storage media from the 1st storage media It checks that the content ID of the contents read from the 1st storage media is not recorded on the invalid content ID managed table of the 1st storage media. Combine the 1st Media ID and content ID of storage media, generate the 1st media content ID, and the contents data of contents are generalized by this 1st media content ID. [1st] While acquiring the purpose information, combine the 2nd Media ID and content ID of storage media, and the 2nd media content ID is generated. [2nd] In order to record the contents which proper-ized the purpose information acquired from the 1st storage media by the 2nd media content ID, generated contents data, and made content ID and contents data the group on the 2nd storage media, The purpose information on the contents currently recorded on the invalid content ID managed table is unacquirable. Therefore, since content ID of contents is made into an invalid in the case of migration when the contents of the 1st storage media are beforehand backed up before migration, Contents cannot be read even if it is going to read and use, as backup is copied to the 1st storage media and mentioned above after migration. In addition, backing up in this case itself has not forbidden. That is, when backup is copied to storage media and returned after contents migration, permitting backup, it is preventing from using these contents.

[0027]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing. Drawing 1 is the block diagram showing the system configuration which enforces the information record approach which makes movable media proper-ized information concerning the 1st operation gestalt of this invention. The system shown in this drawing has the information recording device 2 for recording the purpose information 3, preventing unjust use to the storage media 1 and these storage media 1.

[0028] The storage media 1 have the RAM (ReadOnly Memory) field 14 which are the WAO (Write AtOnce) field 13 which is a peculiar identifier and is a storage region which can be written in only the media ID 11 which are not rewritable, and at once, and a storage region rewritable any number of times for every storage media. The WAO field 13 has the invalid content ID managed table 131.

[0029] Here, the property of the WAO field 13 is explained. Information can be written

in this WAO field 13 only at once. The information written in once cannot be returned. Moreover, the smallest unit of this information to write in is a bit, and can write in information by 1 bitwise.

[0030] An example is given and explained. A 8-bit WAO field is considered. It is "0" at first [all] and all bits can be written in.

[0031] "00000000", next the 4th bit are set to "1." This is possible.

[0032] "00010000" No matter what this "1" may carry out henceforth, it is not made to "0". [bit / 4th] This is the property of a WAO field.

[0033] Furthermore, another bit can be set to "1." For example, it will be set to "00010010" if the 7th bit is set to "1." Thus, if it writes in, all will be soon set to the condition of "1", and "11111111." No matter what it may carry out henceforth, a condition cannot be changed from this condition.

[0034] The RAM field 14 has the available content ID managed table 141 and two or more contents 142. The available content ID managed table 141 backs up contents to others, with the right using contents held, and from the storage media 1, when eliminating contents, it is used in order to prevent using for the storage media 1 after it the content ID of the contents backed up and eliminated to the contents recorded newly. Contents 142 have content ID 1421 and the contents data 1422.

[0035] The information recording apparatus 2 considers two elements of the available content ID 1421 as an input from the storage media 1 to the media ID 11, and the available content ID managed table 141. The media content ID creation means 21 which considers the result of having combined two inputs as an output, A proper-ized means 22 to proper-ize the purpose information 3 by the media content ID outputted from the media content ID creation means 21, It has a contents record means 23 to record the contents 142 which consist of content ID 1421 and contents data 1422 on the RAM field 14. Moreover, the proper-ized means 22 has the equipment key 221.

[0036] Drawing 2 shows the format of the invalid content ID managed table 131. It is a simple bit string and it is shown whether the content ID to which each bit corresponds is invalid. Correspondence with the bit of a table 131 and content ID is matched so that the offset distance from the head of a bit string may be in agreement with the number of content ID. The initial value of the value of a bit is 0 and the bit which corresponds when content ID becomes an invalid is set to 1. The invalid content ID managed table 131 shown in drawing 2 shows that 8 and 13 have invalid content ID. If magnitude of the invalid content ID managed table 131 is set to 16KByte(s), 16x1024x8=131072 piece content ID is manageable. All the initial value of the invalid content ID managed table 131 at the time of shipment of the storage media 1 is 0.

Since the invalid content ID managed table 131 is recorded on the WAO field 13, the bit once set to 1 is never made as for it to 0. Therefore, any content ID cannot be deleted from the invalid content ID managed table 131.

[0037] The format of the available content ID managed table 141 is the same as that of the invalid content ID managed table 131, and the magnitude of a table also makes it the same. All the initial value of the available content ID managed table 141 at the time of shipment of the storage media 1 is 1.

[0038] In addition, in subsequent processings, it means setting the bit in the table corresponding to [recording content ID on a these content ID managed table] the content ID to 1. It means setting the bit in the table corresponding to [deleting content ID from a content ID managed table] the content ID to 0.

[0039] In the 1st operation gestalt constituted as mentioned above, in recording the purpose information C3 on the storage media 1, the media content ID creation means 21 first generates two inputs of the content ID (CI) of a result which searched available content ID from media (MI) ID 11 and the available content ID managed table 141 to media content ID (MCI) from the storage media 1. It is MCI=MI+CI. At this time, content ID (CI) is deleted from the available content ID managed table 141.

[0040] Next, the proper-ized means 22 proper-izes the purpose information C by media content ID, and generates proper-ized information. If the equipment key 221 is set to R, this proper-ized information will be expressed as E (E (R, MCI), C). Finally the contents 142 which used proper-ized information E (E (R, MCI), C) as the contents data 1422 for CI at content ID 1421 are recorded on the RAM field 14 of the storage media 1 with the contents record means 23.

[0041] Drawing 3 is the block diagram showing the system configuration which enforces the information record approach concerning the 2nd operation gestalt of this invention. The system shown in drawing 3 has the storage media 1, the information use equipment 4 which reads information from the storage media 1, and the purpose information 3. The configuration of the storage media 1 is the same as drawing 1 .

[0042] Information use equipment 4 has a contents read-out means 41 to inspect whether the content ID 1421 of the contents 142 which read contents 142 and were further read from the storage media 1 is contained in the invalid content ID managed table 131, the media content ID creation means 43, and a generalization means 42 to generalize the contents data 142 by the media content ID outputted from the media content ID creation means 43. Moreover, the generalization means 42 has the equipment key 421. The equipment key 421 within the generalization means 42 is the same as the equipment key 221 within the above-mentioned proper-ized means 22.

[0043] The case where contents 142 are read from the storage media 1 is explained. In this explanation, the storage media 1 and contents 142 which were written in with the 1st operation gestalt are used. That is, content ID 1421 presupposes that it is CI and the contents data 1422 are E (E (R, MCI), C), and sets media ID 11 to MI. First, with the contents read-out means 41, contents 142 are read and content ID (CI) and the contents data E (E (R, MCI), C) are read. Furthermore, the contents read-out means 41 inspects whether this read content ID (CI) is contained in the invalid content ID managed table 131. When contained, actuation is ended immediately. When not contained, actuation is continued, with the media content ID creation means 43, media content ID (MI+CI=MCI) is generated from content ID (CI) and media ID 11 (MI), the contents data E (E (R, MCI), C) are further generalized by media content ID (MCI) using the generalization means 42, and the purpose information C is acquired.

[0044] Drawing 4 is the block diagram showing the system configuration which enforces the information record approach concerning the 3rd operation gestalt of this invention. The system shown in drawing 4 has information migration equipment 5 which moves information to the storage media B1 from the storage media A1, the storage media B1, and the storage media A1. The configuration of the storage media A1 and B1 is the same as what was shown in drawing 1 and drawing 3 .

[0045] Information migration equipment 5 has the contents read-out means 51, the generalization means 52, the media content ID creation means 53, the proper-ized means 54, and the contents record means 55. The equipment key 521 within the generalization means 52 is the same as the equipment key 541 within the proper-ized means 54.

[0046] The case where contents are moved to the storage media B1 from the storage media A1 is explained. Actuation of the contents read-out means 51, the media content ID creation means 53, and the generalization means 52 carries out the same actuation to the 2nd operation gestalt except for some exceptions. With the exception, the contents read-out means 51 are what (a correspondence bit is set to 0->1) content ID and A1421 are similarly recorded on the invalid content ID managed table A131 for, and that contents A142 are further deleted [what (a correspondence bit is set to 1->0) the read content ID and A1421 are deleted from the available content ID managed table A141 for, and] from the RAM field A14. Thus, the generalization means 52 generates generalization information and passes it to the proper-ized means 54. Hereafter, actuation of the proper-ized means 54, the media content ID creation means 53, and the contents storage means 55 carries out the same actuation as the 1st operation gestalt. Thus, contents B142 are recorded on the storage media B1.

[0047] Drawing 5 is the block diagram showing the system configuration which enforces the information record approach concerning the 4th operation gestalt of this invention. The system shown in drawing 5 has the storage media 1, a backup unit 6, and a magnetic disk 7. It has the contents read-out means 61 and the contents record means 62 in a backup unit 6. In addition, although a part of configuration of the storage media 1 is omitted, it is the same as what was shown in drawing 1 , drawing 3 , and drawing 4 .

[0048] In case backup of contents is taken from the storage media 1 to a magnetic disk 7, the contents read-out means 61 reads contents 142, and records this on a magnetic disk 7. Moreover, when [which copies and returns the data which backed up to the storage media 1 from a magnetic disk 7 (restoration)] carrying out, the contents record means 62 reads data from a magnetic disk 7, and records on the RAM field 14 by making this into contents 142.

[0049] Drawing 6 is the block diagram showing the system configuration which enforces the information record approach concerning the 5th operation gestalt of this invention. The system shown in drawing 6 has deletion equipment 8 with the storage media 1. Deletion equipment 8 has the contents deletion means 81. In addition, although a part of configuration of the storage media 1 is omitted, it is the same as what is shown in drawing 1 , drawing 3 , and drawing 4 .

[0050] When deleting contents 142 from the storage media 1, the contents deletion means 81 reads content ID 1421, deletes this content ID from the available content ID managed table 141, and eliminates contents 142 from the storage media 1.

[0051] When the data of a magnetic disk are restored to the storage media A after the inaccurate user backed up the contents C of the storage media A to the magnetic disk and moved Contents C to another storage media B from the storage media A here, the content ID of the restored contents is recorded on the invalid content ID managed table of Media A. Therefore, these restored contents cannot be read using the information use equipment shown with the 2nd operation gestalt. That is, the unjust use by backup is prevented.

[0052]

[Effect of the Invention] As explained above, according to this invention, combine Media ID and content ID and media content ID is generated. Since the contents which proper-ized the purpose information by media content ID, generated contents data, and made content ID and contents data the group are recorded on storage media While being able to proper-ize the purpose information by the result of having enciphered Media ID by content ID Moreover, it is also possible by preparing another

contents key beforehand, enciphering contents with a contents key, and proper-izing a contents key as purpose information to mitigate processing of encryption of contents.

[0053] moreover, when content ID is recorded on the invalid content ID managed table according to this invention Stop acquisition processing of the purpose information, and when not recorded Since combine Media ID and content ID, media content ID is generated, the contents data of contents are generalized by this media content ID and the purpose information is acquired The purpose information on the contents currently recorded on the invalid content ID managed table can generalize contents data by the result of having enciphered Media ID by content ID further while it is unacquirable.

[0054] Furthermore, in case said contents are moved to the 2nd storage media from the 1st storage media according to this invention It checks that content ID is not recorded on an invalid content ID managed table. Combine the 1st Media ID and content ID of storage media, generate the 1st media content ID, and the contents data of contents are generalized by this 1st media content ID. [1st] Acquire the purpose information, combine the 2nd Media ID and content ID of storage media, and the 2nd media content ID is generated. [2nd] Since the contents which proper-ized the purpose information acquired from the 1st storage media by the 2nd media content ID, generated contents data, and made content ID and contents data the group are recorded on the 2nd storage media The purpose information on the contents currently recorded on the invalid content ID managed table is unacquirable. Therefore, since content ID of contents is made into an invalid in the case of migration when the contents of the 1st storage media are beforehand backed up before migration, Contents cannot be read even if it is going to read and use, as backup is copied to the 1st storage media and mentioned above after migration. That is, although a user can back up, even if it backs up, informational unjust use can be prevented accurately.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the system configuration which enforces the information record approach which makes movable media proper-ized information concerning the 1st operation gestalt of this invention.

[Drawing 2] It is drawing showing a format of the invalid content ID managed table used with the operation gestalt of drawing 1 .

[Drawing 3] It is the block diagram showing the system configuration which enforces the information record approach which makes movable media proper-ized information concerning the 2nd operation gestalt of this invention.

[Drawing 4] It is the block diagram showing the system configuration which enforces the information record approach which makes movable media proper-ized information concerning the 3rd operation gestalt of this invention.

[Drawing 5] It is the block diagram showing the system configuration which enforces the information record approach which makes movable media proper-ized information concerning the 4th operation gestalt of this invention.

[Drawing 6] It is the block diagram showing the system configuration which enforces the information record approach which makes movable media proper-ized information concerning the 5th operation gestalt of this invention.

[Description of Notations]

1 Storage Media

2 Information Recording Device

3 The Purpose Information

4 Information Use Means

5 Information Migration Means

6 Backup Unit

8 Deletion Equipment

11 Media ID

13 WAO Field

14 RAM Field

21 Media Content ID Creation Means

22 Proper-ized Means

23 Contents Record Means

42 52 Generalization means

131 Invalid Content ID Managed Table

141 Available Content ID Managed Table

142 Contents

1421 Content ID

1422 Contents Data

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－298974
（P2000－298974A）
(43)公開日　平成12年10月24日(2000.10.24)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
G11B 27/00		G11B 27/00		5B017
G06F 12/14	320	G06F 12/14	320E	5D110
		G11B 27/00	A	

審査請求　未請求　請求項の数3　ＯＬ　（全 9 頁）

(21)出願番号　特願平11－103130

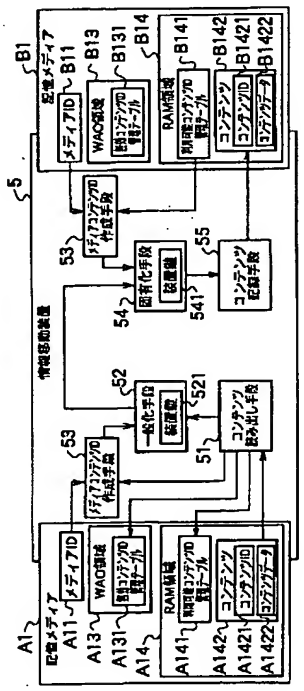
(22)出願日　平成11年4月9日(1999.4.9)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　武井　英明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　曽根岡　昭直
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　メディア固有化情報を移動可能にする情報記録方法

(57)【要約】
【課題】　不正利用を防止しつつ記憶メディアに固有化された情報を他の記憶メディアに移動することを可能にするメディア固有化情報を移動可能にする情報記録方法を提供することにある。
【解決手段】　記憶メディアＡ１から記憶メディアＢ１にコンテンツＡ１４１を移動する際は、コンテンツ読み出し手段５１は記憶メディアＡ１の無効コンテンツＩＤ管理テーブルに読み出したコンテンツＩＤ・Ａ１４２１を記録し、コンテンツデータＡ１４２２は一般化手段５２、固有化手段５４、コンテンツ記録手段５５を経てコンテンツＢ１４２として記憶メディアＢ１に記録し、コンテンツＡ１４２は記憶メディアＡ１から削除する。



【特許請求の範囲】

【請求項１】　一度だけ書き込み可能な記憶領域であるＷＡＯ領域および何度でも書き換え可能な記憶領域であるＲＡＭ領域を有するとともに、メディア毎に固有な識別子である書き換え不可能なメディアＩＤが書き込まれている記憶メディアに対して情報を記録する情報記録方法であって、

前記記憶メディアに目的情報を記録する際は、

前記記憶メディア内で利用できるコンテンツＩＤを検索し、

前記メディアＩＤと前記コンテンツＩＤを結合して、メディアコンテンツＩＤを生成し、

前記目的情報を前記メディアコンテンツＩＤで固有化してコンテンツデータを生成し、

前記コンテンツＩＤと前記コンテンツデータを組にしたコンテンツを前記記憶メディアの前記ＲＡＭ領域に記録することを特徴とするメディア固有化情報を移動可能にする情報記録方法。

【請求項２】　前記記憶メディアにおいて今後使用できないコンテンツＩＤを管理するための無効コンテンツＩＤ管理テーブルを前記ＷＡＯ領域に記録しておき、

前記記憶メディアに記録されている前記コンテンツを読み出し、この読み出したコンテンツから前記目的情報を取得する際は、

前記記憶メディアから読み出した前記コンテンツのコンテンツＩＤが前記無効コンテンツＩＤ管理テーブルに記録されているか否かをチェックし、記録されている場合には、目的情報の取得処理を中止し、

前記コンテンツのコンテンツＩＤが前記無効コンテンツＩＤ管理テーブルに記録されていない場合には、前記メディアＩＤと前記コンテンツＩＤを結合して、メディアコンテンツＩＤを生成し、

この生成したメディアコンテンツＩＤで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得することを特徴とする請求項１記載のメディア固有化情報を移動可能にする情報記録方法。

【請求項３】　前記記憶メディアにおいて今後使用できないコンテンツＩＤを管理するための無効コンテンツＩＤ管理テーブルを前記ＷＡＯ領域に記録しておき、

前記記憶メディアにおいて利用できるコンテンツＩＤを管理するための利用可能コンテンツＩＤ管理テーブルを前記ＲＡＭ領域に記録しておき、

第１の記憶メディアから第２の記憶メディアに前記コンテンツを移動する際は、

前記第１の記憶メディアから前記コンテンツを読み出し、

この読み出したコンテンツのコンテンツＩＤが前記第１の記憶メディアの前記無効コンテンツＩＤ管理テーブルに記録されていないことを確認してから、該コンテンツＩＤを該無効コンテンツＩＤ管理テーブルに記録するとともに、該コンテンツＩＤを前記第１の記憶メディアの前記利用可能コンテンツＩＤ管理テーブルから削除し、

前記第１の記憶メディアの第１のメディアＩＤと前記読み出したコンテンツのコンテンツＩＤを結合して、第１のメディアコンテンツＩＤを生成し、

この第１のメディアコンテンツＩＤで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得し、

前記第２の記憶メディアの第２のメディアＩＤと前記コンテンツＩＤを結合して、第２のメディアコンテンツＩＤを生成し、

前記第１の記憶メディアから取得した目的情報を前記第２のメディアコンテンツＩＤで固有化してコンテンツデータを生成し、

前記コンテンツＩＤと前記コンテンツデータを組にしたコンテンツを前記第２の記憶メディアの前記ＲＡＭ領域に記録し、

前記第１の記憶メディアのＲＡＭ領域に記録されている前記コンテンツを消去することを特徴とする請求項１記載のメディア固有化情報を移動可能にする情報記録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、メディア毎に固有な識別子であるメディアＩＤを有する記憶メディアに対して情報を固有化し、この固有化されている情報を記憶メディアから読み出し、更に他の記憶メディアに移動するとともに情報の不正利用を適確に防止し得るメディア固有化情報を移動可能にする情報記録方法に関する。

【０００２】

【従来の技術】まず、情報の固有化および一般化という用語について説明する。以下では暗号鍵Ｋでデータ Ｄを暗号化することをＥ（Ｋ，Ｄ）と表現する。

【０００３】不正利用を防ぐためによく用いられるのは、情報を記録したり利用する装置間で共有され、かつ利用者には秘密にされている秘密鍵を使う方法である。この秘密鍵のことを装置鍵Ｒと呼ぶ。

【０００４】更に、情報をメディアに固有化することで、情報を他のメディアにコピーしても、他のメディアでは情報を適切に復号化できないため不正利用を防ぐことが可能になる。その１つの例がメディア毎に固有な識別子を利用した方法である。メディア毎に固有な識別子を利用した方法を以下で簡単に説明する。

【０００５】各メディアには、予めメディア毎に固有な識別子（メディアＩＤ）が書き換え可能なように書き込まれている。従って、２つのメディアがあったときに、この２つのメディアのそれぞれのメディアＩＤが一致することはない。このようなメディアに対して不正利用を防止しようとする目的情報Ｃを記録するときには、まずメディアＩＤ（ＭＩ）を装置鍵Ｒで暗号化しＥ（Ｒ，Ｍ

Ｉ）を得る。これを暗号鍵として目的情報Ｃを暗号化して生成される暗号化目的情報Ｅ（Ｅ（Ｒ，ＭＩ），Ｃ）をメディアは書き込むのである。

【０００６】一方この目的情報Ｃを読み出すときには、記録されている暗号化目的情報Ｅ（Ｅ（Ｒ，ＭＩ），Ｃ）とメディアＩＤ（ＭＩ）を読み出し、ＭＩを装置鍵Ｒで暗号化してＥ（Ｒ，ＭＩ）を得て、これを復号鍵としてＥ（Ｅ（Ｒ，ＭＩ），Ｃ）を復号化して目的情報Ｃを得ることができる。

【０００７】このとき、あるメディアＡに記録されている暗号化目的情報を別のメディアＢにコピーし、メディアＢからこの暗号化目的情報を読み出すことを考える。このとき、メディアＡのメディアＩＤ（ＭＩＡ）とメディアＢのメディアＩＤ（ＭＩＢ）は異なる。従って、メディアＢにコピーされた暗号化目的情報を上記のように読み出そうとしても、暗号化に用いた鍵（Ｅ（Ｒ，ＭＩＡ））と復号化に用いる鍵（Ｅ（Ｒ，ＭＩＢ））が異なるため、目的情報を正確に読み出すことはできない。つまりこの暗号化目的情報は、メディアＡに記録されているときのみ有効な情報であり、他のメディアに記録されているときは無効な情報となる。これを目的情報のメディアへの固有化と呼ぶ。情報をメディアに固有化することにより、情報を他のメディアにコピーしても利用することが不可能になり、不正利用を防いでいるのである。

【０００８】また、暗号化目的情報Ｅ（Ｅ（Ｒ，ＭＩ），Ｃ）を生成するには、メディアＩＤ（ＭＩ）と目的情報Ｃの他に装置鍵Ｒを知る必要がある。逆に、暗号化目的情報Ｅ（Ｅ（Ｒ，ＭＩ），Ｃ）を復号化するには、メディアＩＤ（ＭＩ）の他に装置鍵Ｒを知ることが必要になる。従って装置鍵Ｒが秘密に守られているならば、メディアＩＤを知られたからといって、不正に暗号化目的情報を生成したり、暗号化目的情報から目的情報を生成することはできない。

【０００９】以上説明したように、情報をメディアに固有化することは不正利用の防止を実現するのに強力な方法となる。別の言い方をすると、メディア内の情報はそのメディアに固有化されているため、メディア内の情報がたとえコピーされたとしても、それは不正利用防止方法への脅威とはならない。その固有化された情報はそのメディアに記録されているときのみ適切に復号化され意味のあるものになるのであり、他のメディアに記録されているときはまったく無意味なものであるからである。つまりメディアに固有化された情報を利用するためには、そのメディアを物理的に所有する必要がある。情報を利用する権利が物理的なメディアの所有に結び付けられているのである。

【００１０】そこで、メディアＩＤ（ＭＩ）と目的情報Ｃから固有化目的情報Ｅ（Ｅ（Ｒ，ＭＩ），Ｃ）を生成することを目的情報をメディアＩＤで固有化すると表現し、固有化目的情報とメディアＩＤから目的情報を生成することを固有化目的情報をメディアＩＤで一般化すると表現する。

【００１１】以上の説明から明らかなように、メディア内の固有化情報を他のメディアにコピーされても不正利用を防止する上で問題はない。従って利用者はメディア内の固有化情報を例えばハードディスク、ＭＯなどの別のメディアにバックアップとして記録することができる。利用者は、記憶メディア内に多量の情報がたまってきて、残りの記憶容量が少なくなってきたとき、そのうちのいくつかをバックアップとして別の記録媒体にコピーしてとっておき、その記憶メディア内の情報を削除すれば、残りの記憶容量を増やすことができる。必要になればバックアップから記憶メディアに情報をコピーして戻せばよい。戻した情報は有効な情報として利用することが可能である。このように利用者が合法的にいくつでも情報のバックアップをとっておけるということは利用者にとって大変便利なことである。

【００１２】ところで、このような従来の方法では、利用するために記憶メディアに記録してしまった情報を他の記憶メディアで利用するために情報を移動することができず、その点では利用者は不便を強いられてしまう。これはバックアップのことを言っているのではなく、別のメディアに情報をコピーし、その別なメディア上で情報を利用することを許すと不正利用の余地が生まれるということを言っているのである。

【００１３】情報の移動とは、例えばメディアＡからメディアＢに情報を移すことである。利用者は２つのメディアに入っている別々の情報を１つのメディアにまとめることができれば便利であり、このとき情報の移動をすることが必要になる。情報の移動において不正利用を防止するという観点から重要なのは、例えばメディアＡからメディアＢに情報を移すときにメディアＡ内の情報を後から使えないようにするということである。つまり情報の移動とは、メディアＡに固有化されている情報をメディアＢに固有化しなおすという作業であり、移動前はメディアＡと結び付けられていた情報を利用する権利を移動してメディアＢと結び付ける作業であるといえる。

【００１４】メディア間で移動するためには、以下の方法が容易に考えられる。まずメディアＡ内の固有化された情報を一般化する。この一般化された情報をメディアＢに固有化し、メディアＢに記録する。そしてメディアＡ内の固有化された情報を消去する。このような機能を利用者に提供すれば、とりあえず、メディア間の固有化情報の移動が実現できる。

【００１５】しかし、ここで問題となるのは、利用が許されないメディアＡ内の情報が、確実に利用できないようになっているのかということである。例えば利用者が移動の作業をする前にメディアＡ内の情報を予めバックアップしていた場合を考える。移動の作業が終了した後は、メディアＡ内の情報は上記のように消去されるから

確かにメディアＡ内には移動した情報は残っていない。しかし、予めバックアップをとっていたなら、このバックアップをまたメディアＡにコピーして戻してしまえば、この情報は有効であり、利用できるようになってしまう。

【００１６】バックアップを禁止することでこのような不正利用を防止することができるが、バックアップを防止する技術を開発することは、特に単に記録するだけの単純な記憶メディアの場合には困難である。更に、何よりバックアップはそれ自体便利な機能であり、これを禁止することは利用者にとって大変不便である。

【００１７】以上のように、従来の技術では、メディア内の情報を他のメディアに移動する機能を利用者に提供した場合、利用者は情報を不正にコピーして利用することが容易になってしまう。

【００１８】

【発明が解決しようとする課題】上述したように、メディアに固有化された情報を他のメディアに移動させることを実現しようとすると、情報の移動後にバックアップをメディアにコピーしなおすことで容易に不正利用が行われてしまうという問題がある。

【００１９】バックアップを防止することで不正利用を防ぐことができるが、バックアップを防止することは利用者の利便性を損なうという問題がある。

【００２０】本発明は、上記に鑑みてなされたもので、その目的とするところは、記憶メディアに固有化されている情報を異なる記憶メディアに移動することでバックアップを可能にしつつ不正コピーによる情報の不正利用を適確に防止し得るメディア固有化情報を移動可能にする情報記録方法を提供することにある。

【００２１】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、一度だけ書き込み可能な記憶領域であるＷＡＯ領域および何度でも書き換え可能な記憶領域であるＲＡＭ領域を有するとともに、メディア毎に固有な識別子である書き換え不可能なメディアＩＤが書き込まれている記憶メディアに対して情報を記録する情報記録方法であって、前記記憶メディアに目的情報を記録する際は、前記記憶メディア内で利用できるコンテンツＩＤを検索し、前記メディアＩＤと前記コンテンツＩＤを結合して、メディアコンテンツＩＤを生成し、前記目的情報を前記メディアコンテンツＩＤで固有化してコンテンツデータを生成し、前記コンテンツＩＤと前記コンテンツデータを組にしたコンテンツを前記記憶メディアの前記ＲＡＭ領域に記録することを要旨とする。

【００２２】請求項１記載の本発明にあっては、メディアＩＤとコンテンツＩＤを結合してメディアコンテンツＩＤを生成し、目的情報をメディアコンテンツＩＤで固有化してコンテンツデータを生成し、コンテンツＩＤとコンテンツデータを組にしたコンテンツを記憶メディアに記録するため、メディアＩＤをコンテンツＩＤで暗号化した結果で目的情報を固有化し得るとともに、また予め別のコンテンツ鍵を用意し、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を目的情報として固有化することによりコンテンツの暗号化の処理を軽減することも可能である。

【００２３】また、請求項２記載の本発明は、請求項１記載の発明において、前記記憶メディアにおいて今後使用できないコンテンツＩＤを管理するための無効コンテンツＩＤ管理テーブルを前記ＷＡＯ領域に記録しておき、前記記憶メディアに記録されている前記コンテンツを読み出し、この読み出したコンテンツから前記目的情報を取得する際は、前記記憶メディアから読み出した前記コンテンツのコンテンツＩＤが前記無効コンテンツＩＤ管理テーブルに記録されているか否かをチェックし、記録されている場合には、目的情報の取得処理を中止し、前記コンテンツのコンテンツＩＤが前記無効コンテンツＩＤ管理テーブルに記録されていない場合には、前記メディアＩＤと前記コンテンツＩＤを結合して、メディアコンテンツＩＤを生成し、この生成したメディアコンテンツＩＤで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得することを要旨とする。

【００２４】請求項２記載の本発明にあっては、コンテンツのコンテンツＩＤが無効コンテンツＩＤ管理テーブルに記録されている場合には、目的情報の取得処理を中止し、記録されていない場合には、メディアＩＤとコンテンツＩＤを結合してメディアコンテンツＩＤを生成し、このメディアコンテンツＩＤでコンテンツのコンテンツデータを一般化して、目的情報を取得するため、無効になって、無効コンテンツＩＤ管理テーブルに記録されているコンテンツの目的情報は取得できないとともに、更にメディアＩＤをコンテンツＩＤで暗号化した結果でコンテンツデータを一般化することができる。なお、コンテンツに含まれるコンテンツＩＤについては暗号化してなく、コンテンツＩＤを不正に別の値にすることにより、コンテンツを本来のコンテンツＩＤとは別のコンテンツＩＤを有するコンテンツにされる恐れがあるが、コンテンツに含まれるコンテンツデータとしてはコンテンツＩＤを含む値で固有化したデータが記録されており、コンテンツデータはコンテンツＩＤに依存している。この場合、上述したようにコンテンツデータを読み出すときには、本来のコンテンツＩＤでないＩＤを含む値でコンテンツデータを一般化するため、読み出しの結果得られる情報は本当の正直な情報ではなく、無意味な情報となる。従って、コンテンツＩＤを本来のものから変えても得られる情報が無意味になるだけである。

【００２５】更に、請求項３記載の本発明は、請求項１記載の発明において、前記記憶メディアにおいて今後使用できないコンテンツＩＤを管理するための無効コンテ

ンツＩＤ管理テーブルを前記ＷＡＯ領域に記録しておき、前記記憶メディアにおいて利用できるコンテンツＩＤを管理するための利用可能コンテンツＩＤ管理テーブルを前記ＲＡＭ領域に記録しておき、第１の記憶メディアから第２の記憶メディアに前記コンテンツを移動する際は、前記第１の記憶メディアから前記コンテンツを読み出し、この読み出したコンテンツのコンテンツＩＤが前記第１の記憶メディアの前記無効コンテンツＩＤ管理テーブルに記録されていないことを確認してから、該コンテンツＩＤを該無効コンテンツＩＤ管理テーブルに記録するとともに、該コンテンツＩＤを前記第１の記憶メディアの前記利用可能コンテンツＩＤ管理テーブルから削除し、前記第１の記憶メディアの第１のメディアＩＤと前記読み出したコンテンツのコンテンツＩＤを結合して、第１のメディアコンテンツＩＤを生成し、この第１のメディアコンテンツＩＤで前記コンテンツのコンテンツデータを一般化して、前記目的情報を取得し、前記第２の記憶メディアの第２のメディアＩＤと前記コンテンツＩＤを結合して、第２のメディアコンテンツＩＤを生成し、前記第１の記憶メディアから取得した目的情報を前記第２のメディアコンテンツＩＤで固有化してコンテンツデータを生成し、前記コンテンツＩＤと前記コンテンツデータを組にしたコンテンツを前記第２の記憶メディアの前記ＲＡＭ領域に記録し、前記第１の記憶メディアのＲＡＭ領域に記録されている前記コンテンツを消去することを要旨とする。

【００２６】請求項３記載の本発明にあっては、第１の記憶メディアから第２の記憶メディアに前記コンテンツを移動する際は、第１の記憶メディアから読み出したコンテンツのコンテンツＩＤが第１の記憶メディアの無効コンテンツＩＤ管理テーブルに記録されていないことを確認し、第１の記憶メディアの第１のメディアＩＤとコンテンツＩＤを結合して第１のメディアコンテンツＩＤを生成し、この第１のメディアコンテンツＩＤでコンテンツのコンテンツデータを一般化して、目的情報を取得するとともに、第２の記憶メディアの第２のメディアＩＤとコンテンツＩＤを結合して第２のメディアコンテンツＩＤを生成し、第１の記憶メディアから取得した目的情報を第２のメディアコンテンツＩＤで固有化してコンテンツデータを生成し、コンテンツＩＤとコンテンツデータを組にしたコンテンツを第２の記憶メディアに記録するため、無効コンテンツＩＤ管理テーブルに記録されているコンテンツの目的情報は取得できず、従って移動前に予め第１の記憶メディアのコンテンツをバックアップしてあった場合、移動の際にコンテンツのコンテンツＩＤは無効にされるため、移動後にバックアップを第１の記憶メディアにコピーして、上述したように読み出して利用しようとしてもコンテンツを読み出すことはできない。なお、この場合、バックアップすること自体は禁止していない。すなわち、バックアップを許容しつつコンテンツ移動後にバックアップを記憶メディアにコピーして戻した場合に、このコンテンツを利用できないようにしているのである。

【００２７】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図１は、本発明の第１の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。同図に示すシステムは、記憶メディア１、およびこの記憶メディア１に対して不正利用を防止しつつ目的情報３を記録するための情報記録装置２を有する。

【００２８】記憶メディア１は、記憶メディア毎に固有な識別子であって、書き換え不可能なメディアＩＤ１１、一度だけ書き込み可能な記憶領域であるＷＡＯ（Write AtOnce）領域１３、および何度でも書き換え可能な記憶領域であるＲＡＭ（ReadOnly Memory）領域１４を有する。ＷＡＯ領域１３は、無効コンテンツＩＤ管理テーブル１３１を有する。

【００２９】ここで、ＷＡＯ領域１３の性質について説明する。このＷＡＯ領域１３には情報を一度だけ書き込むことができる。一度書き込んだ情報を元に戻すことはできない。また、この書き込む情報の最小単位はビットであり、１ビット単位で情報を書き込むことができる。

【００３０】例をあげて説明する。８ビットのＷＡＯ領域を考える。最初はすべて「０」であり、すべてのビットが書き込み可能である。

【００３１】「００００００００」次に、４ビット目を「１」にしてみる。これは可能である。

【００３２】「０００１０００」この４ビット目の「１」は以後いかなることをしても「０」にできない。これはＷＡＯ領域の性質である。

【００３３】更に別のビットを「１」にすることができる。例えば７ビット目を「１」にすると、「０００１００１０」となる。このようにして書き込みを行っていくと、やがてすべて「１」の状態、「１１１１１１１」になる。この状態からは以後いかなることをしても状態を変化させることはできない。

【００３４】ＲＡＭ領域１４は、利用可能コンテンツＩＤ管理テーブル１４１と複数のコンテンツ１４２を有する。利用可能コンテンツＩＤ管理テーブル１４１は、コンテンツを利用する権利を保持したままコンテンツを他へバックアップし記憶メディア１からはコンテンツを消去してしまう場合に、それ以後に記憶メディア１に新しく記録するコンテンツに対して、バックアップして消去してしまったコンテンツのコンテンツＩＤが使われてしまうことを防ぐために使用される。コンテンツ１４２はコンテンツＩＤ１４２１とコンテンツデータ１４２２を有する。

【００３５】情報記録装置２は、記憶メディア１からメディアＩＤ１１と利用可能コンテンツＩＤ管理テーブル

１４１から利用可能なコンテンツＩＤ１４２１の２つの要素を入力とし、２つの入力を結合した結果を出力とするメディアコンテンツＩＤ作成手段２１と、メディアコンテンツＩＤ作成手段２１から出力されるメディアコンテンツＩＤで目的情報３を固有化する固有化手段２２と、コンテンツＩＤ１４２１とコンテンツデータ１４２２からなるコンテンツ１４２をＲＡＭ領域１４に記録するコンテンツ記録手段２３を有する。また、固有化手段２２は装置鍵２２１を有する。

【００３６】図２は、無効コンテンツＩＤ管理テーブル１３１のフォーマットを示している。単純なビット列であり、各ビットが対応するコンテンツＩＤが無効であるか否かを示している。テーブル１３１のビットとコンテンツＩＤとの対応は、ビット列の先頭からのオフセット距離がコンテンツＩＤの番号と一致するように対応付ける。ビットの値の初期値は０であり、コンテンツＩＤが無効となったとき対応するビットは１にされる。図２に示す無効コンテンツＩＤ管理テーブル１３１では、コンテンツＩＤが８と１３が無効であることを示している。無効コンテンツＩＤ管理テーブル１３１の大きさを１６ＫＢｙｔｅとすると、１６×１０２４×８＝１３１０７２個のコンテンツＩＤを管理することができる。記憶メディア１の出荷時における無効コンテンツＩＤ管理テーブル１３１の初期値はすべて０である。無効コンテンツＩＤ管理テーブル１３１はＷＡＯ領域１３上に記録されるため、一度１にしたビットは二度と０にできない。従って、無効コンテンツＩＤ管理テーブル１３１からはいかなるコンテンツＩＤも削除できない。

【００３７】利用可能コンテンツＩＤ管理テーブル１４１のフォーマットは無効コンテンツＩＤ管理テーブル１３１と同一であり、テーブルの大きさも同じとする。記憶メディア１の出荷時における利用可能コンテンツＩＤ管理テーブル１４１の初期値はすべて１である。

【００３８】なお、以降の処理において、これらコンテンツＩＤ管理テーブルにコンテンツＩＤを記録するとは、そのコンテンツＩＤに対応するテーブル中のビットを１にすることを意味する。コンテンツＩＤ管理テーブルからコンテンツＩＤを削除するとは、そのコンテンツＩＤに対応するテーブル中のビットを０にすることを意味する。

【００３９】以上のように構成される第１の実施形態において、目的情報Ｃ３を記憶メディア１に記録する場合には、まずメディアコンテンツＩＤ作成手段2.1によって記憶メディア１からメディアＩＤ（ＭＩ）１１と、利用可能コンテンツＩＤ管理テーブル１４１から利用可能なコンテンツＩＤを検索した結果のコンテンツＩＤ（ＣＩ）の２つの入力から、メディアコンテンツＩＤ（ＭＣＩ）を生成する。ＭＣＩ＝ＭＩ＋ＣＩである。このときコンテンツＩＤ（ＣＩ）は利用可能コンテンツＩＤ管理テーブル１４１から削除する。

【００４０】次に、固有化手段２２が目的情報Ｃをメディアコンテンツ ＩＤで固有化して固有化情報を生成する。装置鍵２２１をＲとすると、この固有化情報は、Ｅ（Ｅ（Ｒ，ＭＣＩ），Ｃ）と表現される。最後にＣＩをコンテンツＩＤ１４２１に、固有化情報Ｅ（Ｅ（Ｒ，ＭＣＩ），Ｃ）をコンテンツデータ１４２２としたコンテンツ１４２をコンテンツ記録手段２３によって記憶メディア１のＲＡＭ領域１４に記録する。

【００４１】図３は、本発明の第２の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図３に示すシステムは、記憶メディア１と、記憶メディア１から情報を読み出す情報利用装置４と、目的情報３を有する。記憶メディア１の構成は図１と同じである。

【００４２】情報利用装置４は、記憶メディア１からコンテンツ１４２を読み出し、更に読み出したコンテンツ１４２のコンテンツＩＤ１４２１が無効コンテンツＩＤ管理テーブル１３１に含まれているかどうかを検査するコンテンツ読み出し手段４１と、メディアコンテンツＩＤ作成手段４３と、メディアコンテンツＩＤ作成手段４３から出力されるメディアコンテンツＩＤでコンテンツデータ１４２を一般化する一般化手段４２を有する。また、一般化手段４２は装置鍵４２１を有する。一般化手段４２内の装置鍵４２１は前述の固有化手段２２内の装置鍵２２１と同一である。

【００４３】記憶メディア１からコンテンツ１４２を読み出す場合について説明する。この説明では第１の実施形態で書き込んだ記憶メディア１とコンテンツ１４２を用いる。すなわち、コンテンツＩＤ１４２１はＣＩ、コンテンツデータ１４２２はＥ（Ｅ（Ｒ，ＭＣＩ），Ｃ）であるとし、メディアＩＤ１１はＭＩとする。まず、コンテンツ読み出し手段４１によってコンテンツ１４２を読み出し、コンテンツＩＤ（ＣＩ）とコンテンツデータＥ（Ｅ（Ｒ，ＭＣＩ），Ｃ）を読み出す。更にコンテンツ読み出し手段４１は、この読み出したコンテンツＩＤ（ＣＩ）が無効コンテンツＩＤ管理テーブル１３１に含まれていないか検査する。含まれていた場合には、ただちに動作は終了となる。含まれていない場合は、動作を続行し、メディアコンテンツＩＤ作成手段４３によって、コンテンツＩＤ（ＣＩ）とメディアＩＤ１１（ＭＩ）からメディアコンテンツＩＤ（ＭＩ＋ＣＩ＝ＭＣＩ）を生成し、更に一般化手段４２を用いて、コンテンツデータＥ（Ｅ（Ｒ，ＭＣＩ），Ｃ）をメディアコンテンツＩＤ（ＭＣＩ）で一般化し、目的情報Ｃを得る。

【００４４】図４は、本発明の第３の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図４に示すシステムは、記憶メディアＡ１と、記憶メディアＢ１と、記憶メディアＡ１から記憶メディアＢ１に情報を移動する情報移動装置５を有する。記憶メディアＡ１，Ｂ１の構成は図１、図３に示したものと同

じである。

【００４５】情報移動装置５はコンテンツ読み出し手段５１と、一般化手段５２と、メディアコンテンツＩＤ作成手段５３と、固有化手段５４と、コンテンツ記録手段５５を有する。一般化手段５２内の装置鍵５２１は固有化手段５４内の装置鍵５４１と同一である。

【００４６】記憶メディアＡ１から記憶メディアＢ１にコンテンツを移動する場合を説明する。コンテンツ読み出し手段５１、メディアコンテンツＩＤ作成手段５３、一般化手段５２の動作は、第２の実施形態と一部の例外を除き同一の動作をする。その例外とは、コンテンツ読み出し手段５１は読み出したコンテンツＩＤ・Ａ１４２１を利用可能コンテンツＩＤ管理テーブルＡ１４１から削除する（対応ビットを１→０にする）ことと、同じくコンテンツＩＤ・Ａ１４２１を無効コンテンツＩＤ管理テーブルＡ１３１に記録する（対応ビットを０→１にする）こと、更にコンテンツＡ１４２がＲＡＭ領域Ａ１４から削除されることである。このようにして、一般化手段５２は一般化情報を生成し、固有化手段５４に渡す。以下、固有化手段５４、メディアコンテンツＩＤ作成手段５３、コンテンツ記憶手段５５の動作は、第１の実施形態と同一の動作をする。このようにして、コンテンツＢ１４２が記憶メディアＢ１に記録される。

【００４７】図５は、本発明の第４の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図５に示すシステムは、記憶メディア１と、バックアップ装置６と、磁気ディスク７を有する。バックアップ装置６にコンテンツ読み出し手段６１と、コンテンツ記録手段６２を有する。なお、記憶メディア１の構成は、一部省略されているが、図１、図３、図４に示したものと同じである。

【００４８】記憶メディア１から磁気ディスク７にコンテンツのバックアップをとる際は、コンテンツ読み出し手段６１がコンテンツ１４２を読み出し、これを磁気ディスク７に記録する。また、磁気ディスク７から記憶メディア１にバックアップしたデータをコピーして戻す（リストア）する場合は、コンテンツ記録手段６２が磁気ディスク７からデータを読み出し、これをコンテンツ１４２としてＲＡＭ領域１４に記録する。

【００４９】図６は、本発明の第５の実施形態に係る情報記録方法を実施するシステム構成を示すブロック図である。図６に示すシステムは、記憶メディア１と、削除装置８を有する。削除装置８はコンテンツ削除手段８１を有する。なお、記憶メディア１の構成は、一部省略されているが、図１、図３、図４に示すものと同じである。

【００５０】記憶メディア１からコンテンツ１４２を削除する場合は、コンテンツ削除手段８１がコンテンツＩＤ１４２１を読み出し、このコンテンツＩＤを利用可能コンテンツＩＤ管理テーブル１４１から削除し、コンテンツ１４２を記憶メディア１から消去する。

【００５１】ここで不正利用者が記憶メディアＡのコンテンツＣを磁気ディスクにバックアップし、コンテンツＣを記憶メディアＡから別の記憶メディアＢに移動した後、磁気ディスクのデータを記憶メディアＡにリストアした場合には、リストアしたコンテンツのコンテンツＩＤはメディアＡの無効コンテンツＩＤ管理テーブルに記録されている。従って第２の実施形態で示した情報利用装置を使ってこのリストアされたコンテンツを読み出すことはできない。つまり、バックアップによる不正利用は防がれているのである。

【００５２】

【発明の効果】以上説明したように、本発明によれば、メディアＩＤとコンテンツＩＤを結合してメディアコンテンツＩＤを生成し、目的情報をメディアコンテンツＩＤで固有化してコンテンツデータを生成し、コンテンツＩＤとコンテンツデータを組にしたコンテンツを記憶メディアに記録するので、メディアＩＤをコンテンツＩＤで暗号化した結果で目的情報を固有化し得るとともに、また予め別のコンテンツ鍵を用意し、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を目的情報として固有化することによりコンテンツの暗号化の処理を軽減することも可能である。

【００５３】また、本発明によれば、コンテンツＩＤが無効コンテンツＩＤ管理テーブルに記録されている場合には、目的情報の取得処理を中止し、記録されていない場合には、メディアＩＤとコンテンツＩＤを結合してメディアコンテンツＩＤを生成し、このメディアコンテンツＩＤでコンテンツのコンテンツデータを一般化して、目的情報を取得するので、無効コンテンツＩＤ管理テーブルに記録されているコンテンツの目的情報は取得できないとともに、更にメディアＩＤをコンテンツＩＤで暗号化した結果でコンテンツデータを一般化することができる。

【００５４】更に、本発明によれば、第１の記憶メディアから第２の記憶メディアに前記コンテンツを移動する際は、コンテンツＩＤが無効コンテンツＩＤ管理テーブルに記録されていないことを確認し、第１の記憶メディアの第１のメディアＩＤとコンテンツＩＤを結合して第１のメディアコンテンツＩＤを生成し、この第１のメディアコンテンツＩＤでコンテンツのコンテンツデータを一般化して、目的情報を取得し、第２の記憶メディアの第２のメディアＩＤとコンテンツＩＤを結合して第２のメディアコンテンツＩＤを生成し、第１の記憶メディアから取得した目的情報を第２のメディアコンテンツＩＤで固有化してコンテンツデータを生成し、コンテンツＩＤとコンテンツデータを組にしたコンテンツを第２の記憶メディアに記録するので、無効コンテンツＩＤ管理テーブルに記録されているコンテンツの目的情報は取得できず、従って移動前に予め第１の記憶メディアのコンテ

ンツをバックアップしてあった場合、移動の際にコンテンツのコンテンツＩＤは無効にされるため、移動後にバックアップを第１の記憶メディアにコピーして、上述したように読み出して利用しようとしてもコンテンツを読み出すことはできない。すなわち、利用者はバックアップすることはできるが、バックアップしたとしても情報の不正利用は適確に防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図２】図１の実施形態で使用される無効コンテンツＩＤ管理テーブルのフォーマットを示す図である。

【図３】本発明の第２の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図４】本発明の第３の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

【図５】本発明の第４の実施形態に係るメディア固有化情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

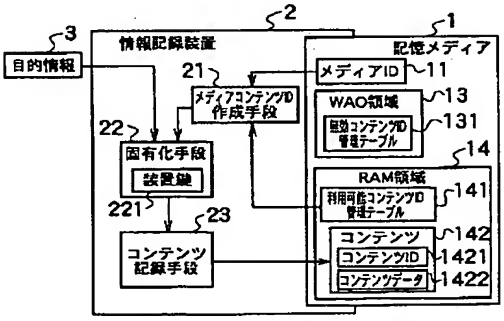
【図６】本発明の第５の実施形態に係るメディア固有化＊

＊情報を移動可能にする情報記録方法を実施するシステム構成を示すブロック図である。

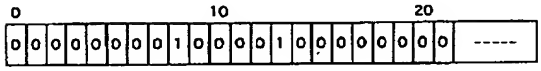
【符号の説明】

１　記憶メディア
２　情報記録装置
３　目的情報
４　情報利用手段
５　情報移動手段
６　バックアップ装置
８　削除装置
１１　メディアＩＤ
１３　ＷＡＯ領域
１４　ＲＡＭ領域
２１　メディアコンテンツＩＤ作成手段
２２　固有化手段
２３　コンテンツ記録手段
４２，５２　一般化手段
１３１　無効コンテンツＩＤ管理テーブル
１４１　利用可能コンテンツＩＤ管理テーブル
１４２　コンテンツ
１４２１　コンテンツＩＤ
１４２２　コンテンツデータ

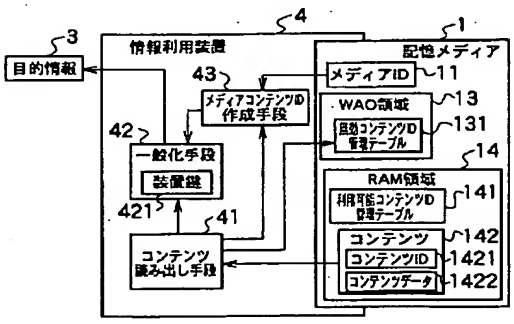
【図１】



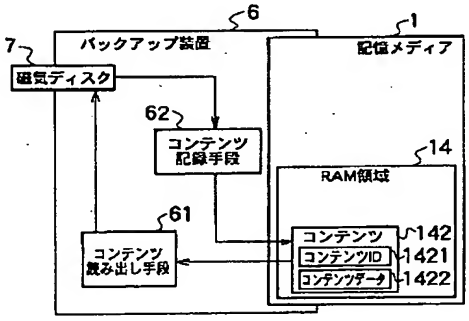
【図２】



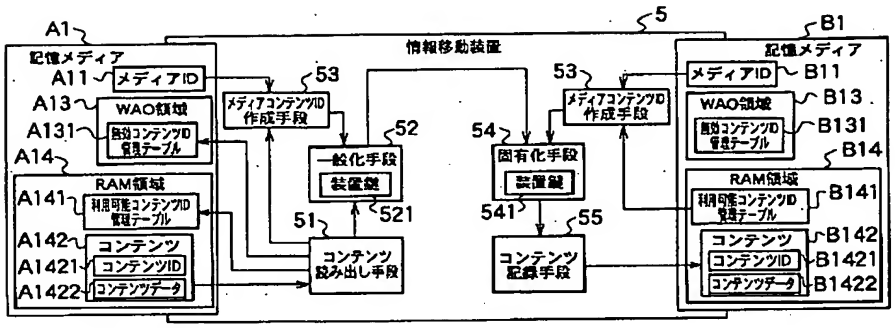
【図３】



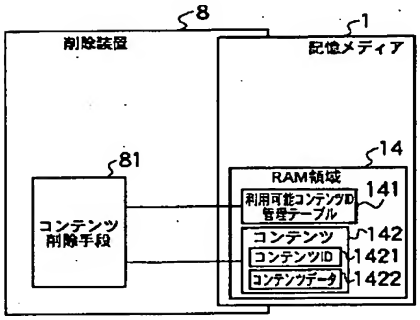
【図５】



【図４】



【図６】



フロントページの続き

Ｆターム(参考) 5B017 AA06 BA05 BA07 CA06 CA11
CA16
5D110 AA16 AA17 DA02 DA11 DB03
DC28 DD13 DD16 DE04